

CLAIMS

What is claimed is:

1 1. A computerized method for restricting network access by applications comprising:
2 detecting a network access request from an application;
3 examining an application policy file to determine if the application is authorized to
4 access the network; and
5 blocking access to the network if the application is not authorized to access the
6 network.

1 2. The method of claim 1 further comprising:
2 determining a network resource requested by the application;
3 examining the application policy file to determine if the application is authorized to
4 access the network resource; and
5 allowing access to the network resource if the application is authorized to access
6 the network resource.

1 3. The method of claim 1 further comprising:
2 determining a type of network access requested by the application;
3 examining the application policy file to determine if the application is authorized
4 for the type of network access requested; and
5 allowing the type of network access requested if the application is authorized for
6 the type of network access requested.

1 4. The method of claim 1 further comprising:
2 updating the application policy file; and
3 re-evaluating applications currently executing against the updated policy file.

1 5. The method of claim 1 further comprising:
2 determining if the application is allowed access to the network based on an
3 application identifier in the network access request.

1 6. The method of claim 1, wherein the method is performed on a client computer on
2 which the application is executing.

1 7. A computer-readable medium having executable instruction to cause a computer to
2 perform a method comprising:

3 detecting a network access request from an application;
4 examining an application policy file to determine if the application is authorized to
5 access the network; and
6 blocking access to the network if the application is not authorized to access the
7 network.

1 8. The computer-readable medium of claim 7, wherein the method further comprises:
2 determining a network resource requested by the application;
3 examining the application policy file to determine if the application is authorized to
4 access the network resource; and
5 allowing access to the network resource if the application is authorized to access
6 the network resource.

1 9. The computer-readable medium of claim 7, wherein the method further comprises:
2 determining a type of network access requested by the application;
3 examining the application policy file to determine if the application is authorized
4 for the type of network access requested; and
5 allowing the type of network access requested if the application is authorized for
6 the type of network access requested.

1 10. The computer-readable medium of claim 7, wherein the method further comprises:
2 updating the application policy file; and
3 re-evaluating applications currently executing against the updated policy file.

1 11. The computer-readable medium of claim 7, wherein the method further comprises:
2 determining if the application is allowed access to the network based on an
3 application identifier in the network access request.

1 12. A computer system comprising:
2 a processing unit;
3 a memory coupled to the processing unit through a bus;
4 a network interface coupled to the processing unit through the bus and further
5 operable for coupling to a network; and
6 an application policy process executed from the memory by the processing unit to
7 cause the processing unit to detect a network access request from an application, to
8 examine an application policy file to determine if the application is authorized to access
9 the network, and to block access to the network if the application is not authorized to
10 access the network.

1 13. The computer system of claim 12, wherein the application policy process further
2 causes the processing unit to determine a network resource requested by the application, to
3 examine the application policy file to determine if the application is authorized to access
4 the network resource, and to allow access to the network resource if the application is
5 authorized to access the network resource.

1 14. The computer system of claim 12, wherein the application policy process further
2 causes the processing unit to determine a type of network access requested by the
3 application, to examine the application policy file to determine if the application is

4 authorized for the type of network access requested, and to allow the type of network
5 access requested if the application is authorized for the type of network access requested.

1 15. The computer system of claim 12, wherein the application policy process further
2 causes the processing unit to update the application policy file, and to re-evaluate
3 applications currently executing against the updated policy file.

1 16. The computer system of claim 12, wherein the application policy process further
2 causes the processing unit to determine if the application is allowed access to the network
3 based on an application identifier in the network access request.

1 17. The computer system of claim 12, wherein the application is executed from the
2 memory by the processing unit.

1 18. A computer-readable medium having stored thereon an application policy data
2 structure comprising:
3 an application identifier field containing data identifying an application;
4 a network identifier field containing data identifying a entity that is accessible by
5 the application identified by the application identifier field; and
6 an access flag field containing data specifying whether the application identified by
7 the application identifier field is allowed access to the entity identified by the network
8 identifier field.

1 19. The computer-readable medium of claim 18 further comprising:
2 an additional policy rule field containing data specifying whether the application
3 identified by the application identifier field is allowed a particular type of access to the
4 entity identified by the network identifier field.

- 1 20. The computer-readable medium of claim 18 further comprising:
 - 2 a response field containing data specifying an action to be performed if the application
 - 3 identified by the application identifier field attempts access to the entity identified by the
 - 4 network identifier field and the access is not allowed.
 - 1 21. The computer-readable medium of claim 18, wherein the entity is selected from the
 - 2 group consisting of a network and a network resource.